



PROJECT MUSE®

Law, Liberty, and the Pursuit of Terrorism

Douglas, Roger

Published by University of Michigan Press

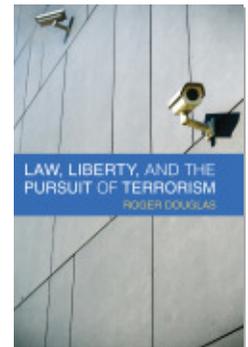
Douglas, Roger.

Law, Liberty, and the Pursuit of Terrorism.

University of Michigan Press, 2014.

Project MUSE., <a href="

<https://muse.jhu.edu/>.



➔ For additional information about this book

<https://muse.jhu.edu/book/36854>

Access provided at 2 Apr 2020 02:13 GMT with no institutional affiliation



This work is licensed under a [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by-nc-nd/4.0/).

Protecting Government Secrets While Protecting Due Process?

People hide from government, and government hides from the people, and people and government have both good and bad reasons for hiding from each other.

*Richard Posner*¹

[W]here secrecy reigns, we naturally suspect that unsavoury things go on in the shadows.

*Thomas Poole*²

The obverse of government interest in others' secrets is a government interest in protecting its own secrets. Laws afford less protection to government secrets than they once did, but they still provide considerable protection for secrets with national security implications, and terrorism has generally been recognised as a threat to national security. Nonetheless, national security interests no longer trump all other interests, and to varying degrees, they must compete against conflicting public and private interests, particularly due process interests. Much of the relevant law predates recent terrorism concerns, but some of it reflects recent attempts by lawmakers to devise arrangements for accommodating the conflicting interests at play.

One area where these conflicts have proved inescapable has been in relation to judicial and quasi-judicial proceedings. The political arms have attempted to devise procedures that protect secrets while affording a degree of due process. Courts continue to recognise governments' interests in keeping secrets, but protecting secrecy normally comes at a price: governments may not normally base their case on evidence unless they are also prepared to disclose it to the opposing party. Moreover, if a secret could help exculpate a criminal defendant, the government may be required to choose between disclosure and discontinuing the prosecution. In US civil cases, the protection of state secrets tends to trump the interests of nonstate plaintiffs. If the success of a nonstate plaintiff requires the disclosure of a state secret, the court will not permit the case to proceed if either the government is unable to defend or

the plaintiff is unable to prove its case other than by the disclosure of the secret. In the other four countries considered in this book, security interests are to be weighed against interests in fair trial, but a plaintiff's interest in being able to pursue a meritorious claim may sometimes mean that governments are required either to disclose the secret or to concede the plaintiff's case.

Terrorism concerns have inspired attempts to enhance protections for government secrets, but the relevant post-9/11 legislation has generally been unambitious. It has largely built on pre-9/11 precedents rather than seeking to overturn established principles, and it has aroused far less passion than attempts to enhance governments' surveillance powers. Courts have shown some deference to executive assessments of national security needs, especially in the United States. But deference has coexisted with unwillingness to accept legislative innovations whose effect is to threaten established due process rights, as well as a reluctance to accept government secrecy claims in the absence of evidence to sustain them. This is an area of law where courts tend to get their way, with constitutional norms to draw on and opportunities for executive deviance limited. Political differences have left a limited legacy, with the role of party being mediated by the exigencies of holding office.

Laws

Counterterror measures have generated a large volume of litigation, which typically requires that governments provide evidence to support their claims (when they want to take coercive action) and their defences (when plaintiffs contend that they are entitled to damages as a result of government misconduct). Fairness also dictates that if the government is in possession of evidence that would assist defendants or civil litigants, it should disclose it. This can pose problems for governments. Sometimes the problem is that the evidentiary basis for state action has been flimsy, and sometimes it is that the government does indeed possess information that undermines its case. But sometimes the disclosure of evidence may be objectionable on more-defensible grounds. Evidence may disclose the identity of informants and thereby imperil their security, undermine their capacity to provide further useful information, and encourage other potential informants to have second thoughts. Evidence may throw light on surveillance procedures and capacities, thereby enabling terrorists to take steps to reduce their vulnerability. Apparently innocuous pieces of information may lead to the uncovering of well-kept secrets.

These dangers can be exaggerated and need to be kept in proportion. Successful counterterror activities must almost invariably disclose some information of use to terrorists, and if they leave no mark, this too may be use-

ful information. If every piece of a potential mosaic must be kept secret, this must necessarily be at the cost of the suppression of much innocuous information. Given the ease with which secrets can be stolen and broadcast, there is much to be said for using them while they last. Sometimes the disclosure of information may serve useful purposes. While knowledge of how antiterrorism agencies work may enable terrorists to adjust, it may also discourage timid would-be terrorists who learn, for instance, that the member of the group who advocates militant action may well be the undercover operative assigned to the group or that they have attracted official interest, in which case their value as a terrorist may be limited. Moreover, like antiterrorist agencies, courts need information if they are to do their job properly.

Someone has to decide how to handle these conflicting considerations. Legislatures have made some contribution by devising a variety of arrangements designed to protect interests in both fair trial and security. But on the whole, the relevant law has been developed by or within a framework settled by courts.

What Secrets Are Protected?

In the United States, secrets are protected from disclosure if their disclosure would threaten national security.³ It is for the court to decide whether a secret involves “matters which, in the interest of national security, ought not be disclosed”; once the court finds the condition is satisfied, the information is privileged.⁴ However, though the courts have overriding power, they defer. Writing in 2005, Weaver and Pallitto claimed that there had never been a case “where courts have forced the government to disclose agency-held classified information in any case in which the privilege has been asserted.”⁵ Yet a secret is not a state secret simply because the executive wants to protect it, Supreme Court authority to this effect being a legacy of Richard Nixon’s shenanigans.⁶

In the other jurisdictions, “crown privilege,” the equivalent to the state secrets privilege, has generally been subsumed within “public interest immunity.” This means that while national security interests carry considerable weight, the national security interest in any given case must be weighed against a countervailing public interest in disclosure, and the logic of the balancing test is that there may be circumstances where a national security interest should be sacrificed in favour of the interest in fair trial. Moreover, courts are concerned not only with the balance between disclosure and secrecy but with whether it is possible to achieve an optimal balance by orders for partial disclosure.⁷

In Canada, Australia, and New Zealand, public interest immunity is now

regulated by post-9/11 legislation. In general, this codifies the common law, but it involves slight modifications.⁸ Amendments made to the Canada Evidence Act by the Anti-terrorism Act 2001 empower the attorney general to respond to a disclosure order by issuing a certificate prohibiting disclosure in security-sensitive cases. Such orders are reviewable by a single federal judge, but only on the basis that some or none of the information “does not relate either to information obtained in confidence from, or in relation to a foreign entity . . . , or to national defence or security.”⁹ The legislation means that national security can trump any countervailing interest in disclosure. However, in criminal cases, courts retain the power to determine the consequences of a decision to withhold evidence.¹⁰ As of March 2007, no such certificates appear to have been issued, and a search of CanLII has not thrown up any subsequent examples.¹¹ Australian legislation maintains the balancing requirement, defines what is entailed in “prejudice to national security,” but requires that the court give “greatest” weight to security interests.¹² The New Zealand Evidence Act 2006 specifies categories of state secrets that qualify for protection, but it otherwise codifies the common law.

Procedures for Determining Whether Information Qualifies for Protection

Decisions as to whether alleged secrets should be disclosed require inquiry into whether an alleged secret warrants any protection and, if so, what. Conducting this inquiry in open court and in the presence of all parties would defeat the purpose of the inquiry if disclosure of the alleged secret really would threaten the national interest. Under largely superseded law, the question of whether a secret qualified for protection was generally resolved on the basis of a certificate from a senior official, with minimal inquiry into the basis for the certificate. The government must now show that there is a basis for its claim, usually supported by evidence, though considerable deference is given to government claims.¹³ In the United States, courts generally resolve disclosure issues without examining documents embodying the secrets in question,¹⁴ and elsewhere courts may but need not base their decisions on an affidavit rather than on an actual examination of the document.¹⁵

Insofar as courts take their role seriously, inquiries into whether information should be protected are complex, especially when they also involve taking account of the public interest in a fair trial and the question of what forms of partial disclosure might represent optimal compromises between conflicting public interests. If what turn out to be protection-worthy secrets are to be protected, procedures are needed to ensure that the process that leads to this

determination does not simultaneously lead to their disclosure. Preliminary inquiries (and freedom of information inquiries for that matter) are therefore governed by procedures that are far less open than those governing trials.

In several jurisdictions, the handling of disputes about the admissibility of secrets is governed by legislation. In the United States, Canada, and Australia, legislation requires notification to the government of the possibility that protected information will be disclosed in the course of a criminal trial (United States)¹⁶ or a criminal or civil trial (Canada, Australia).¹⁷ The legislation also governs the procedures for determining whether and to what extent secrets will be protected. These procedures are similar to those that apply under the general law in other jurisdictions.

The general rule is that disputes about the admissibility of secret information take place in the presence of all parties except insofar as the protection of potentially secret information requires the absence of parties to the dispute. Courts have a right to full access to the information but potentially lack the assistance that could be provided by nongovernment parties and their counsel. This obviously assists the government. It seems unfair, and it deprives the court of submissions that might enable it to reach a more informed decision, but it is unavoidable if secrets are to be protected. This problem predates terrorism concerns; indeed, it is a problem that can arise in relation to purely private litigation, when commercial and other private secrets are implicated in litigation. Legislatures and courts have adopted a number of partial solutions.

One solution involves the use of security-cleared counsel. Australian law makes express provision for security-cleared counsel, and in the United States, protective orders made under the Classified Information Procedures Act of 1980 may and do make provision for security-cleared counsel.¹⁸ The rationale for requiring security clearance lies in the assumption that security-cleared lawyers will be less likely than other lawyers to disclose state secrets. Security clearance is not lightly granted, and once granted, it is not lightly put at risk.

Another solution involves the appointment of “special advocates.” The special advocate procedure appears to have been a Canadian invention,¹⁹ but it first received legislative recognition in the United Kingdom, where legislation provides for its use in relation to several special terrorism jurisdictions.²⁰ At the suggestion of the Canadian Supreme Court, Canada subsequently legislated to make provision for special advocates in cases involving security certificates in relation to immigrants suspected of constituting security risks.²¹ In New Zealand, special advocates were used on an ad hoc basis to deal with the secrecy problems involved in determining whether Ahmed Zaoui had been properly determined to be a security risk (and therefore potentially deport-

able), and there is now statutory provision for the use of special advocates in immigration matters.²² Courts in the United Kingdom and Australia have ruled that special advocates can be used in relation to proceedings in the ordinary courts.²³ In Canadian civil litigation, court-appointed security-cleared “*amici curiae*” have been used in closed hearings to determine whether information should be disclosed,²⁴ and US and Australian courts have concluded that they could appoint experts to perform a similar function.²⁵

Under UK law, special advocates differ from security-cleared advocates in that once they have seen the secret material, they may normally have no further communication with the party whose interests they are representing.²⁶ This potentially deprives them of information relevant to whether the secret should be disclosed, but it is intended to avoid an alternative danger: namely, that a communication informed by awareness of the secret may inadvertently involve the direct or indirect disclosure of the secret. In Canada, courts may grant advocates leave to question the person on whose behalf they are acting, and the experience of Canadian advocates is that this can sometimes be helpful in uncovering exculpatory information.²⁷

Yet another possible solution would involve reliance on the integrity of counsel, whether cleared or not. Given the professional costs of being found to have disclosed confidential information, lawyers will not lightly betray confidences, but politically committed counsel may be tempted to do so, especially in cases where proof of their involvement might be difficult,²⁸ and politically uncommitted counsel might do so inadvertently.²⁹ Nonetheless, “uncleared” counsel have sometimes been used in sensitive cases.³⁰

The Consequences of Nondisclosure

In criminal law cases, the law is reasonably straightforward and varies little across jurisdictions. If the protected information would otherwise have assisted the government, the government is no longer able to rely on it to prove its case. This means that the protection of secrets may sometimes come at the cost of the government’s ability to secure convictions. If disclosure of the secret would strengthen the defendant’s case or weaken the case of the prosecution, the government must make concessions that ensure that the defendant is not seriously disadvantaged. If this is not possible, proceedings will be stayed. However, the government can withhold secrets if their exculpatory potential is no more than theoretical.

If it is the defendant who wants to disclose a state secret, a nondisclosure order might mean that the defendant could not present a defence that might otherwise be open. This would be unfair, and a court would normally order a

stay. However, it would not do so if it concluded that the order did not materially affect the defendant's capacity to present a defence.

In several jurisdictions, legislation expressly permits partial disclosure in the form of summaries or admissions of facts that the information would tend to prove.³¹ In the United Kingdom, Canada, and Australia (but not in the United States), witnesses may give evidence without their identity being disclosed, from behind a screen, or with their voice scrambled, and the duty to disclose seems slightly narrower.³² However, US courts have managed to devise procedures designed to provide some protection to the interests of witnesses and security, and in certain circumstances, their identity may be kept secret.³³ Moreover, courts recognise that the unfairness associated with non-disclosure of protected information may be slight, in which case a trial may be allowed to proceed, notwithstanding a possibility that unfairness might be occasioned by exclusion of the evidence.

These considerations mean that in criminal cases, the distinction between state secrets immunity and public interest immunity is of limited practical significance. Cases in which disclosure would be ordered under the former but not the latter, system would normally be cases where defendants' interests in a fair trial would be adversely affected, in which case courts would order that proceedings be discontinued on fairness grounds.

In civil proceedings, a finding that information is protected means that if a party can make out its claim or defence only by disclosing a state secret, the claim must be dismissed.³⁴ If the plaintiff cannot sustain its case without the evidence, the defendant wins. If the defendant is unable to mount a defence that would otherwise be open to it, the claim will be struck out as an abuse of process.³⁵ The practical consequences of this are potentially unjust, especially in the United States, where the public interest in a plaintiff being able to make out what would otherwise be its case carries no weight in determining whether information can be withheld. Elsewhere, security interests carry considerable weight but are capable of being outweighed by the public interest in plaintiffs being able to pursue their legal interests. It is rare to find cases where governments have succeeded in having cases struck out after having successfully asserted public interest immunity.³⁶

In none of the jurisdictions is there provision for disclosure to the court but not to one or more parties, and this seems to be the case even if selective disclosure in a particular case might be in the public interest. In an interlocutory ruling in a UK torture case, the Queen's Bench Division was willing to allow some classified information to be disclosed to the court, with the plaintiffs' interests being protected by a special advocate,³⁷ but the court of appeal and (with one dissent) the Supreme Court allowed the plaintiffs' appeal, reaffirming the principle that evidence be disclosed to

all parties or to none.³⁸ If there were to be such a departure from tradition, this should be a matter for the Parliament.³⁹ The Supreme Court was not asked to consider whether parties could agree to a closed procedure, with judges expressing different views.⁴⁰ Lord Brown concluded that the problem posed by the case was beyond the courts' capacity to resolve and that such cases either should be tried by a specialist body such as the Investigatory Powers Tribunal (which hears complaints against allegedly unlawful interception of communications) or should not be tried at all. But it was for the Parliament to decide how to deal with the problem, not the courts.⁴¹ Canadian courts have adverted to the question and hinted that closed evidence might be admissible, but in *Canada (Attorney General) v Almallki*, the federal court warned that it could not be assumed that protected information could be disclosed *ex parte*, citing the UK court of appeal's *Al Rawi v Security Service* decision.⁴²

The rules governing public law cases are more complex and vary cross-nationally and by subject matter. There is one important difference between public law and other cases: courts may sometimes rely on secret information, even if this is not communicated to the party seeking relief. In the Guantánamo cases, the courts recognised this principle, subject to the requirement that applicants be provided with enough information to enable them to know the case they had to rebut.⁴³ In the United Kingdom, the court of appeal in *Al Rawi* assumed that there were circumstances where courts could proceed *ex parte* in public law cases, but the Supreme Court disagreed.⁴⁴ The Supreme Court did, however, recognise that legislation permitting closed hearings in private and public law cases could be compatible with the ECHR. The basis for its decision was that the common law was more exacting than the convention.⁴⁵

Australian legislation dating from 1998 envisaged that courts conducting reviews of ministers' decisions in migration cases might make orders that confidential material be disclosed to neither applicants nor their counsel, notwithstanding that it had been disclosed to the court.⁴⁶ The Australian Federal Court based its decision in *Leghaie*⁴⁷ largely on secret information that was communicated to the applicant's security-cleared lawyer and not to his client, but this procedure had had the parties' agreement.

The rationale for *ex parte* use of secrets appears to lie in the fact that it may be the lesser of two evils.⁴⁸ The applicant in a security-related public law case may be able to win only if the court has access to the protected information. If so, the applicant is better off if the court receives it *ex parte* than if it does not receive it at all. If the applicant wins, there is no injustice to the defendant, since the defendant—the government—can be told why it has lost in a classified judgment.

Specialised Courts and Tribunals

Slightly different laws govern specialised courts and tribunals established to deal with terrorism and national security issues. Some of these predate 9/11. In the United States, the Foreign Intelligence Surveillance Act of 1978 includes provisions enabling determinations to be made in relation to whether electronic surveillance has been unlawful, and it includes procedures for dealing with cases where a determination of this issue might involve the disclosure of information when this would be harmful to national security. In these circumstances, the attorney general may file an affidavit that disclosure or an adversary hearing would harm national security. If so, and notwithstanding any other law to the contrary, the question shall be determined by the relevant district court in camera and ex parte. The court may nonetheless disclose to the aggrieved person “portions of the application, order, or other materials,” but only if subject to “appropriate security procedures and protective orders” and only “where the disclosure is necessary to make an accurate determination of the legality of the surveillance.”⁴⁹ In a 2003 decision, the Seventh Circuit reported that it had found no case in which a court had ordered disclosure of FISA materials, and the government brief submitted in a 2008 case asserted that this was still so.⁵⁰

The legislation governing listing decisions under the International Emergency Economic Powers Act of 1977 and the designation of organisations as “foreign terrorist organizations” includes provisions governing the judicial review of designation decisions, including express provision to the effect that for the purposes of in camera and ex parte review, the government might submit classified information used in the making of the designation decision.⁵¹

The post-9/11 administrative arrangements governing Combatant Status Review Tribunals (CSRTs) and military commissions empowered the relevant bodies to act on information not disclosed to the detainee.⁵² Detainees were entitled to attend proceedings, but not when the proceedings involved “testimony or other matters that would compromise national security if heard in the presence of the detainee.” Their personal representatives—security-cleared military officers—were permitted to attend all stages of the proceedings except those in which the members of the tribunal deliberated and voted.⁵³ They were not permitted to share classified information with detainees, but, unlike UK special advocates, they were permitted to communicate with the detainee after having seen confidential material.⁵⁴ The order establishing military commissions allowed the accused to be privately represented (at their own expense), but their civilian lawyer had no right to know the contents of classified material. Access to classified material was subject to rules similar to those governing CSRTs.⁵⁵ Legislation enacted in the aftermath of

*Hamdan v Rumsfeld*⁵⁶ shifted the balance away from the government. The Military Commissions Act of 2006⁵⁷ included provisions for protecting classified information, making it “privileged from disclosure if disclosure would be detrimental to national security.”⁵⁸ In relevant cases, the military judge might order, as an alternative to the production of sensitive information, partly redacted documents, the substitution of a summary of the relevant evidence, or the substitution of a statement of relevant facts that the evidence would tend to prove.⁵⁹ In 2009, these provisions were replaced by provisions modeled on but slightly different to those in the Classified Information Protection Act.⁶⁰ The new provisions provide for discovery of classified information or an adequate substitute, if the information “would be noncumulative, relevant, and helpful to a legally cognizable defense, rebuttal of the prosecutor’s case, or to sentencing,” and the provisions expressly provide that all information admitted as evidence must be disclosed to the accused, who may be ordered not to disclose the information insofar as it is classified.⁶¹ The commission may authorise the government to rely on redacted material, statements, or summaries, but only if these “will provide the defendant with substantially the same ability to make his defense as would disclosure of the original material.”⁶²

A series of UK acts established courts to deal with a variety of security-related issues, including appeals from immigrants found to pose an unacceptable security risk, appeals by and on behalf of proscribed organisations, employment disputes giving rise to security issues, cases arising under surveillance legislation, and applications for the making or review of control orders and their successors.⁶³ Proscribed organisation hearings are governed by the same rules of evidence as those governing civil actions.⁶⁴ The rules of the Special Immigration Appeals Commission require the tribunal to ensure that information not be disclosed contrary to “the interests of national security, the international relations of the United Kingdom, the detention and prevention of crime, or in any other circumstances where disclosure is likely to harm the public interest,” and they provide that parties may be excluded from parts of a hearing.⁶⁵ The rules governing employment tribunals, surveillance appeals, and control orders and measures under the Terrorism Prevention and Investigation Measures Act 2011 are similar.⁶⁶ In such cases, the relevant minister or a party to the proceeding may request that the attorney-general appoint a special advocate.⁶⁷

Canadian migration legislation provides for special procedures in cases where immigrants are appealing against deportation and detention on security grounds following ministerial certification. As enacted, the legislation required a judge hearing a certificate appeal to hear evidence in camera and ex parte, if the judge concluded that “its disclosure would be injurious to national security or to the safety of any person.”⁶⁸ A similar provision governed

the review of decisions to list bodies as terrorist entities and to certify that charities were making contributions to listed entities.⁶⁹

In migration cases (but not in terrorist entity cases), the judge was to provide the applicant with a summary of the grounds for the certificate, but the summary was not to include any information whose disclosure would, in the judge's opinion, damage national security or threaten any person's safety.⁷⁰ There was no provision for anyone to represent the applicant in closed hearings. Following the Supreme Court's decision in *Charkaoui v Canada (Citizenship and Immigration)*, the legislation made provision for the appointment of a special advocate, whose role is almost identical to that of the UK special advocates but whose powers to communicate with the represented person are greater.⁷¹

Australian law makes many of the commonwealth's administrative decisions reviewable on their merits by the Administrative Appeals Tribunal, a court-like body with a comprehensive jurisdiction. Under pre-9/11 legislation, the attorney-general may certify that information should not be divulged on security grounds, in which case it may be disclosed only to the tribunal.⁷² Similar rules govern appeals to the Migration Review Tribunal, but in refugee cases, certification also precludes disclosure to the Refugee Review Tribunal.⁷³ Certificates are not conclusive: being administrative decisions, they are judicially reviewable.

This contrasts with the position under New Zealand's recently proclaimed *Immigration Act 2009*, which includes provisions designed to protect security-sensitive information while minimally detracting from immigrants' due process rights. While the legislation allows the Immigration and Protection Tribunal and courts to examine classified information that has been withheld from the immigrant, its status may be contested by special advocates and others, and it may be taken into account only if the immigrant whose interests are at stake can be given the gist of the adverse allegation without endangering the secret.⁷⁴

Legislation as a Response to Terrorism?

Secrets laws were clearly modified in response to terrorism concerns, but responses tend not to fit the model of heightened concern. First, many of the post-9/11 responses were neither passed nor introduced in the immediate aftermath of the attacks. Indeed, much of the relevant law predates the 9/11 attacks. Second, much of the post-9/11 legislation was based on legislation passed prior to the attacks.

Canada comes closest to providing prima facie evidence of panic-based

legislation. The Anti-terrorism Act 2001 expanded the government's powers to protect its secrets in judicial proceedings, provided for in camera and ex parte hearings in cases challenging terrorist organisation decisions, and included a new official secrets act. It provided for the attorney general to issue certificates prohibiting the disclosure of security-sensitive information. These would be conclusive as against the information and privacy commissioners in relation to whether information fell within the security exemption.

However, despite the speed with which the legislation was passed, it was considered by House and Senate committees that conducted hearings and made or recommended amendments. The Canadian House of Commons Standing Committee on Justice and Human Rights reported the bill subject to amendments that limited the life of the attorney general's certificates to 15 years (under the bill's first reading, they had been indefinite), required publication of certificates, and provided for their judicial review.⁷⁵ The Senate committee recommended further amendments (which, however, were not adopted).⁷⁶

Moreover, the legislation has survived reconsideration. Five years after the passage of the legislation, two parliamentary committees inquired into and reported on the legislation. A Senate committee recommended that provision be made for the involvement of special advocates in all cases where the government sought to rely on secret evidence and that the provisions for ministerial certificates be tightened.⁷⁷ These recommendations could suggest second thoughts, but they reflect concerns similar to those articulated by the Senate committee that had considered the 2001 bill. The House of Commons subcommittee also recommended a special advocate system (but one that placed more emphasis on counsel's duty to the public than on the applicant/defendant's interest). It had only minor reservations about the ministerial certificate system.⁷⁸ But the Parliament adopted almost none of these recommendations, and the one recommendation it did adopt was a response not to the recommendations but to a subsequent Supreme Court decision.

The most important limits on Australian litigants' access to security-related information are those relating to tribunal proceedings, and these predate the 9/11 attacks and have not been amended in response to them. The 2004-5 legislation governing the use of security-sensitive information in criminal and civil trials is procedural rather than substantive, and debates on the bill made few specific references to its implications for counterterrorism.

Most of the relevant UK law predates 9/11, and the only significant post-2001 measures there drew on earlier precedents in which information was kept secret, the affected parties' interests being partly protected by use of special advocates. The US Congress has been even more restrained. While parts

of the Military Commissions Acts are controversial, and while the 2006 act was partly enacted against the backdrop of the forthcoming elections,⁷⁹ its provisions in relation to the protection of state secrets in commission trials do not suggest either haste or capitulation to short-term heightened concern. It was prompted not by terrorist attacks but by a Supreme Court decision holding that the existing system of military commissions was unlawful. However, reconsideration produced legislation that has slightly increased the protections afforded defendants in cases where secrets are relevant to prosecutions and defences.

Institutional Differences

Courts are necessarily involved in secrecy issues. Terrorism-related trials mean that courts are necessarily involved in the need to make decisions in relation to whether secrets are at stake and with what implications. Moreover, statutory secrets provisions have constitutional implications. In Canada, where legislation gives federal judges the jurisdiction to make admissibility decisions, federalism issues arise when the relevant litigation takes place in provincial courts. Legislation that limits courts' access to otherwise admissible evidence and that directs courts in relation to the weight they are to give to security interests raises issues of separation of powers. Ex parte hearings raise due process issues. Deferential courts may welcome the excuse to dispose of politically controversial cases on state secrets grounds, but even relatively cautious courts may be uneasy about rules of law that stand in the way of their resolving cases on their legal and factual merits.

Courts and State Secrets Claims

Courts have been extremely receptive to state secrets claims by the US government. *Reynolds v United States* continues to live a charmed life, in contrast to other questionable wartime decisions that have either been distinguished (like *Johnson v Eisentrager*) or disowned (like *Korematsu v United States* or the UK analogue *Liversidge v Anderson*, which has been overruled). Weaver and Palitto found that state secrets claims failed in only 4 out of 58 reported cases in the period 1977–2005—twice because it was obviously inapplicable, once because of failure to follow procedural prerequisites, and once because the court decided to deal with the problem by ordering a secret trial.⁸⁰ Post-2005 claims have enjoyed a similar level of success, which has generally assisted the government's substantive objectives. In relation to National Security Agency litigation, the government enjoyed mixed success, winning in a case where

the doctrine was found to be fatal to the plaintiffs' standing in a claim for declaratory and injunctive relief,⁸¹ losing in a case where the court held that state secrets privilege was superseded by the special procedures governing FISA damages claims,⁸² and losing on a dismissal application on the grounds that it had not shown that the plaintiffs would have to rely on state secrets in order to make out their case.⁸³ However, the government has been more successful in torture and unlawful rendition cases, including cases where some doubt existed as to whether claims would require the disclosure of state secrets.⁸⁴

Two of the plaintiffs to the US torture litigation were also involved in litigation in the United Kingdom, where they were far more successful. One set of cases related to Binyam Mohamed's application for an order that the United Kingdom produce documents in its possession relating to his mistreatment in the United States, which might assist him in relation to a US habeas corpus application. His application succeeded at first instance, but subject to public interest immunity.⁸⁵ Judgment was given in both open and closed forms, the former giving somewhat less detail about the nature of Mohamed's "cruel, inhuman and degrading" treatment in Pakistan. The question of which, if any, documents had to be disclosed was never resolved: the United States subsequently made the documents available, so there was no need for the United Kingdom to do so. However, an ongoing issue related to whether the open judgment should have included the redacted passages. Concerned that full disclosure would mean the disclosure of information provided by American intelligence agencies, the UK government was worried that if the information was disclosed—even under court order—the US would be worried about the precedent this would create and would be more cautious about the kind of intelligence it would provide in future. There was a political principle at stake, notwithstanding that the gist of the information had been disclosed in the judgment. The trial judge was sceptical of this claim and decided that redaction was no longer appropriate.

The court of appeal held, albeit with some hesitation, that the trial judge had erred. He should not have assumed that there was no danger the disclosure would undermine the flow of intelligence simply because, in a communication intended for a court, the Central Intelligence Agency had been tactful in the way it had adverted to possible consequences.⁸⁶ He had failed to recognise that "at least on the face of it, the Foreign Secretary, with the benefit of his Foreign Office and SyS and SIS advisers, is better able to assess that risk than a judge."⁸⁷ He had not taken into account the secretary's argument that disclosure of the information might also affect the willingness of countries other than the US to provide such information,⁸⁸ and he had erred in his handling of information about the US secretary of state's expressed views.⁸⁹ De-

spite these criticisms, the court considered that there were good grounds for being sceptical of the secretary's claims, albeit on grounds not quite sufficient for finding in favour of disclosure.

But since the divisional court's decision, there had been a change in circumstances. A decision by the DC district court had vindicated Mohamed's claims of torture and mistreatment. The information in the redacted passages was now in the public domain and, moreover, had been disclosed by an arm of the government that had supplied the intelligence. It had ceased to be secret, and there was no longer any rational basis for determining that disclosure would threaten national security.

Binyam Mohamed and Al Rawi also succeeded in a claim for rendition-related damages brought in the UK courts, although the precise nature of and basis for this success is unclear. Following the ruling that the government could not rely on secret evidence, the court ordered the first stage of the discovery process, the giving of a list of relevant documents. This did not resolve the question of whether listed documents would attract public policy immunity. That would await inspection of hundreds of thousands of relevant documents, and the government anticipated that this would keep platoons of lawyers at work for years. There are reports that the case has been settled on terms under which the plaintiffs would receive sums of up to around one million pounds. The security service was reportedly fearful lest claims for public policy immunity would fail, so that its secrets would be disclosed.⁹⁰ But other plausible hypotheses include fear lest the government lose, fear lest an adverse precedent in relation to liability for complicity be established, and concerns at the cost to a financially straitened government if the case were to proceed. Given the cost of conducting the public interest immunity inquiry, the government was probably better off by 10 to 15 million pounds than it would have been had it fought and won.

In Canada, government claims to public interest immunity have sometimes carried little weight with courts. In litigation relating to whether the Arar Commission's investigation into the treatment of a Canadian who had been subject to extraordinary rendition could disclose information allegedly prejudicial to national security, Justice Noël rejected some of the government's claims, and the information was subsequently released. The justice's unclassified reasons set out the principles governing his decision, though not their application, but their logic is that the government was overclaiming.⁹¹ Following the more-rigorous disclosure requirements prescribed in 2008 by the Supreme Court in *Charkaoui v Canada (Citizenship and Immigration)*, Mr. Charkaoui finally achieved substantive success in his attempt to have an adverse security certificate set aside when the designated federal judge rejected

a government claim to public interest immunity and ordered disclosure of the information in question. Rather than disclose its secrets, the government decided that it would not present security-sensitive evidence to the judge.⁹² It conceded that the effect of withdrawing the evidence was that there was no longer sufficient evidence to support the certificate, which was accordingly declared void from the date the material was withdrawn.⁹³ Courts handling Canada's unlawful rendition cases have yet to determine whether any information attracts immunity and, if so, what consequences follow. The plaintiffs will no doubt be encouraged by UK developments. However, the government had one partial success. In *Canada (Attorney General) v Khawaja*,⁹⁴ Justice Moseley upheld all its claims to the effect that disclosure of contested information would be prejudicial to national security, although he also concluded that the interests of justice required disclosure of some of the particulars of the protected information.

Australian law is kinder to governments, although not as kind as governments might wish. In a case arising out of adverse security assessments, ASIO failed in a claim that it was not required to provide an affidavit of documents in response to a discovery notice. However, the Federal Court of Australia (in which discovery is discretionary) also observed that circumstances might arise when national security interests might warrant refusal to order the listing of sensitive documents.⁹⁵ The court subsequently held that ASIO was not required to produce the documents, even to the applicants' lawyers, and that this was the case notwithstanding that this might make it impossible for the applicants to make out their cases.⁹⁶ It subsequently denied the judicial review application.⁹⁷ A case of complicity in torture was settled before the Federal Court had an opportunity to make a public ruling on the public interest immunity issues posed by the litigation.

In the only litigation arising out of a New Zealand security risk certificate, the courts effectively resolved the dispute without having to determine whether there were adequate grounds for the certificate. They found that even if there were grounds for the certificate, the subject of the certificate could not be deported if this would entail refoulement to a country where he would be tortured.⁹⁸ As a refugee from Algeria, he was safe.

The Validity of Procedures for Deciding Whether Secrets Can Be Withheld

In relation to interlocutory disputes as to whether the information ought to be excluded, courts have accepted that they have no alternative but to handle the dispute in camera and ex parte, but even this practice has caused con-

cern insofar as it may involve the judge becoming aware of facts that are not disclosed to the nonstate party. The ECtHR has ruled that in these circumstances, the ECHR requires that criminal defendants excluded from the inquiry be given notice of the gist of any prejudicial material in cases where the judge conducting the inquiry is also the trial judge, and the court came close to ruling that this was so even in the case of jury trials.⁹⁹ Elsewhere, courts have been less concerned about the possibility that exposure to secrets could contaminate judicial minds. In general, however, the problem is mitigated by the role of security-cleared counsel or special advocates.

In Canada, the 2001 amendments to the Canada Evidence Act gave rise to a different issue. On their face, the amendments give the federal court the exclusive jurisdiction to resolve disclosure issues, even in relation to proceedings being litigated before a provincial superior court.¹⁰⁰ This overcomes objections based on judges being prejudiced by virtue of exposure to secret information, but it raised the question of whether the legislation impermissibly interferes with the prerogatives of provincial superior courts by removing their decision-making powers in relation to executive claims that particular evidence is privileged. Several provincial superior courts held that this was the case, at least in some circumstances. The Supreme Court disagreed, ruling that the bifurcated system is constitutionally valid insofar as it applies to criminal cases.¹⁰¹ A claim based on the Canadian Constitution failed: the Constitution protected only such powers as were vested in provincial courts at the time of its enactment, and in 1867, provincial courts lacked the power to determine issues of crown privilege. The legislation did not interfere with a core judicial function or with the charter right to a fair trial. The basis for its decision in relation to the latter two issues was that, properly interpreted, the legislation required courts to take all steps possible to ensure that privilege decisions did not interfere with a defendant's right to a fair trial and that if, for some reason, a fair trial could not be had, the court could protect the defendant's rights by staying proceedings, a right acknowledged by the legislation. While the need for the federal court to make decisions in relation to evidence in matters being tried in provincial courts might complicate proceedings and render them potentially unfair, it did not interfere with the courts' power to order a stay in such circumstances. The legislation might be unwise, but it did not require that defendants be tried other than fairly.¹⁰²

This reasoning does not necessarily apply to civil law, where the salutary effects of a threatened stay would be irrelevant in cases where the defendant was a government agency or official. Nonetheless, provincial courts have held that the bifurcated system is constitutionally valid insofar as it applies at the interlocutory stage.¹⁰³ The Ontario Court of Appeal reversed a ruling by the motion judge that the legislation was invalid in relation to the resolu-

tion of evidence issues once trial had begun, but it did so on the grounds that the ruling was premature since the proceedings had not yet reached that stage.¹⁰⁴

The Validity of Legislative Attempts to Limit the Circumstances in Which Secrets Can Be Disclosed in Judicial Proceedings

Legislation designed to make it easier for the government to exclude secret information raises fairness and accuracy issues. At worst, the legislation dealing with ordinary criminal and civil trials only slightly nibbles away at the principle that as much probative evidence as possible should be admissible, and it has survived judicial scrutiny. Canadian courts have dismissed challenges to the validity of legislation permitting the attorney general to issue a (judicially reviewable) certificate precluding the disclosure of security-sensitive information. The Supreme Court's judgment in *Charkaoui v Canada* included dicta that strongly implied that the Evidence Act provisions were unexceptionable,¹⁰⁵ and in the course of the tortuous *Khawaja* litigation, the federal court¹⁰⁶ and the federal court of appeal¹⁰⁷ rejected challenges to the constitutionality of the legislation. The legislation did not deprive the accused of his right to a trial in accordance with the principles of fundamental justice, which varied with circumstances and might require taking account of state interests as well as individual interests. Moreover, the legislation expressly provided for the dismissal or stay of criminal charges if denial of access to information meant that the defendant could not receive a fair trial.

The Supreme Court's recent decision in *R v Ahmad* seems less deferential. It made it clear that the bifurcated system was valid only because it permits courts to engage in rigorous examination of privilege claims, and there is a hint that section 38.13 (whose validity was not at issue in *Ahmad*) might be constitutionally suspect.¹⁰⁸ Except in relation to the bifurcated decisions issue, courts have not, however, considered the implications of the amendments in the context of civil or public law trials. The logic of *Ahmad* is that there should be no problems as long as the fairness of the trial is unaffected and that constitutional difficulties could arise if the government attempted to use section 38.13 to its advantage.

The Australian National Security Information (Criminal and Civil Proceedings) Act 2004 (NSIA) has survived constitutional challenge, partly because it left the powers of the courts largely unaffected. Although it required courts to give greater weight to security interests than to other interests, this was not held to involve an impermissible interference with constitutionally protected judicial powers.¹⁰⁹ There has, however, been a hint that its definition of "national security" may be overbroad.¹¹⁰

The Validity of Measures Allowing the Ex Parte Use of Secrets in Trials and Inquiries

Quite different issues arise where governments want the court to take account of secrets while keeping them concealed from the nonstate parties. To allow this may mean breaching a fundamental principle of procedural fairness, namely, the right of people to know the case they need to meet. Moreover, the lack of an informed response to the secret evidence means that there is a danger that the court will lack some of the information it needs to make an informed decision. Legislation that allows the state to rely on secret information is therefore in danger of falling foul of constitutionally protected due process rights. Anticipating this problem, most statutory regimes attempt to provide some protection for the nonstate party. The United Kingdom relied heavily on special advocates. The United States and Australia rely on security-cleared counsel. Where the secret is such that nonstate parties can be put on notice as to the case they must meet, due process concerns become less serious. The problem is, however, that the essence of the secret may be crucial and may be what the government wants to keep secret. For example, governments naturally want to keep the identity of informants secret, but keeping identity secret means that the subject of the information may not be in a position to advance persuasive reasons for why the tribunal should attach little weight to superficially persuasive evidence. The UK special advocate procedure does not work well in such a situation, given bars on contacts with the nonstate party following examination of the closed material. Security-cleared counsel are in a slightly better position, but their duty not to disclose secrets sets limits to the questions they can ask their clients (and, indeed, to their right to knowingly allow their eyes to light up when their client spontaneously points out that if the adverse information came from a named person, who the lawyer knows to be the confidential source, there are good reasons why it should be treated as lacking in credibility).

Legislation allowing the ex parte communication of evidence to tribunals has survived constitutional scrutiny insofar as it applies to decisions designating groups and individuals as terrorists, but not (except in minor respects) in relation to the determination of combatant status. A USA Patriot Act amendment provided that in judicial reviews of determinations made under section 2003 of the International Emergency Economic Powers Act, classified information might be submitted to the reviewing court ex parte and in camera.¹¹¹ Courts have consistently upheld the constitutionality of this amendment, on the basis that the powers are conditioned on the measures being necessary for the protection of national security, and they have also upheld similar restrictions on challenging designation as a “foreign terrorist organization.”¹¹²

In the United States, litigation put in question the legality of the CSRTs and the military commissions. In *Hamdan*, the Supreme Court held that the military commissions were inconsistent with the Uniform Code of Military Justice and the Geneva Conventions and that Congress could legislate to confer the relevant authority.¹¹³ In *Boumediene v Bush*, the Supreme Court left open the question of whether the CSRT procedures satisfied due process requirements, but the majority concluded that “there is a considerable risk of error in the tribunal’s findings of fact.”¹¹⁴ It held, however, that the combination of the CSRT procedures and the statutory provisions for judicial review of CSRT decisions¹¹⁵ fell short of providing the procedural protections needed to justify legislation depriving detainees of their constitutional right to apply for habeas corpus. The Supreme Court’s concerns included the detainees’ limited access to information about the evidence against them.

However, the procedures designed to deal with subsequent Guantánamo habeas corpus litigation involved acceptance of the need to provide some protection for government secrets. This had been recognised in 2004, when the DC district court recognised petitioners’ rights to habeas corpus but made orders to protect government secrets. Following *Boumediene*, the DC district court made a protective order superseding its earlier orders (Protective Order 08),¹¹⁶ which it amended in January 2009.¹¹⁷ The government was entitled to refuse to disclose classified information if it could provide a sufficient alternative. If it could not provide a sufficient alternative, it could withhold the information, but if so, the court might make orders in the nature of those provided for under the Classified Information Protection Act.¹¹⁸ Access to classified information was limited to the government and to security-cleared counsel who had signed the prescribed memorandum of understanding. They were permitted to discuss it with other security-cleared counsel in related cases but were not to disclose it to a detainee except with permission.

UK courts have been wary of allowing courts and specialised tribunals to act on secret information. Most of the relevant litigation has related to whether rights to fair trial for those subjected to control orders are adequately protected by the special advocate system. When the House of Lords first dealt with the question, it concluded that the special advocate system was potentially capable of ensuring a fair trial, notwithstanding that the controllee had not been made aware of the contents of the closed material. However, disclosure to the special advocate would not necessarily mean that a control order hearing would be fair, and the rules had to be read down accordingly.¹¹⁹

The ECtHR subsequently took a stricter approach, disagreeing with the decision by the House of Lords insofar as it accepted that failure to disclose the full nature of the government’s case was not necessarily contrary to the ECHR’s provisions for fair trial,¹²⁰ and the House of Lords had no alternative

but to follow.¹²¹ These rulings did not require that the party be given access to all confidential information, but they did require that a party subject to a control order be given details of the gist of the case against it, such that it would be in a position to respond to all allegations against it. If this requirement was satisfied, a control order could be made, notwithstanding that the party was not aware of the full details of the evidence produced against it. If it could not be satisfied, the government was not permitted to rely on the evidence.

However, both the ECtHR and the Supreme Court have held that the demands of fair trial were less exacting when liberty interests were not engaged.¹²² Among the issues involved in *Kennedy v United Kingdom* was the question of whether the procedures used by the Investigatory Powers Tribunal were consistent with the requirements of Convention Articles 6 (fair hearing) and 13 (right to effective remedy): the restrictions on the applicant's right were both necessary and proportionate.¹²³ A subsequent Supreme Court case arose from the Home Office's withdrawal of a security clearance. The employee argued that it had discriminated against him on impermissible grounds. Following an application by the Home Office, the Employment Tribunal made an order for a closed material procedure. This meant that some evidence would be heard in the absence of the employee and that the employee might not be given enough details of the evidence to be able to make an effective response. His interests would, however, be represented by a special advocate. The Supreme Court held that this procedure did not contravene the ECHR. There was European authority permitting security interests to prevail over disclosure, even if this came at some cost to the person's capacity to rebut and to their ability to know the precise reasons for an adverse decision. The court was sensitive to the dangers of forcing governments to choose between disclosing information and being unable to sustain a meritorious case, and the court accepted that security vetting was both desirable and dependent on confidential sources. However, the closed material procedure was valid only because of safeguards, which included the tribunal's discretion to determine whether to make the order and the discretion to make orders whose practical effect might be the disclosure of security-sensitive information. But while there was agreement as to the need for balance, there was disagreement as to its extent. Lords Brown and Hope appear to have been particularly sensitive to the need to protect the vetting system. Lord Kerr, who dissented in part, was sensitive to procedural fairness issues, finding that procedural fairness required that the employee be provided with the gist of the closed evidence, even if this might interfere with the effectiveness of the vetting system.

Canadian courts have reached a similar conclusion in relation to legislation governing immigrants suspected of being potential terrorists. In *Charkaoui v Canada*,¹²⁴ the Supreme Court unanimously held that section 78 of the

Immigration and Refugee Protection Act infringed section 7 of the Canadian Charter of Rights and Freedoms, which provides that people may be deprived of life, liberty, and security only in accordance with the principles of fundamental justice. The court made it clear that this did not mean that applicants were entitled to access to the evidence, but it did mean that there should be provision for someone to make representations to the court on the applicant's behalf in such matters. The model suggested was the special advocate one, and the legislature duly obliged. In a subsequent decision,¹²⁵ the court considered the degree of disclosure required in relation to the issue of a ministerial certificate and held that the charter rights of a person affected by such a decision were such that they should be afforded similar rights to a criminal defendant, subject to public interest immunity considerations. However, a subsequent federal court challenge to the amended legislation was unsuccessful, Justice Noël finding that the new procedure did not offend against the charter's provisions for fair trial and, further, that even if it had done so, it would have been "demonstrably justifiable in a free and democratic society" and therefore saved by section 1 of the charter.¹²⁶

While the Australian Constitution does not include a due process clause, legislative attempts to require courts to follow unfair procedures would contravene the constitutionally based separation of powers. Those affected by administrative decisions have a presumptive right to procedural fairness, but the existence and content of that right is subject to legislation. As a result, in cases where a person's status is affected by adverse security assessments, courts have consistently held that the subject of the certificate has no right to know the nature of the information on which it is based, except insofar as its disclosure would not threaten security interests.¹²⁷ High Court litigation relating to the government's right to detain would-be immigrants who had been found to be security risks did not resolve the question of whether legislation could limit the procedural fairness rights of those affected by adverse security assessments. The court found that ASIO had in fact afforded procedural fairness to the plaintiffs in that it had informed them of the gist of the allegations against them and given them an opportunity to reply.¹²⁸

The Executive and Government Secrets

The history of the relevant legislation indicates that government attempts to enhance their secrecy powers are usually watered down in the legislative process and that legislative opposition to secrecy legislation is invariably on the grounds that secrecy should not receive any more protection than it currently enjoys. However, judging by the fate of their legislative proposals, governments generally secured most of what they wanted, which suggests either that

their moves for legislation were particularly opportune or that governments and legislatures are broadly agreed as to the advantages of both state secrecy and open government.

But agreement might also reflect government calculations about what might be politically feasible, and in the United States, the government's response to secrecy concerns in relation to counterterrorism tended to take the form of executive unilateralism rather than attempts to extract protective legislation. Its procedures for determining combatant status and guilt of war crimes were designed to ensure that secrets could be both used and kept and that detainees would be hard-pressed to show that they were not properly detained and innocent of the charges against them. Its use of executive powers to protect its secrets was also evidenced by measures designed to limit access to information. In an October 2001 memorandum, Attorney General Ashcroft urged a policy of presumptive nondisclosure in relation to any information that might be confidential, promising the Department of Justice's support for nonrelease decisions other than those that lacked a "sound legal basis" or that frustrated the capacity of other agencies to protect their records. Officials responded by becoming less likely to release information.¹²⁹ The government resisted attempts by civil liberties and other organisations to gain access to information relating to details of post-9/11 immigration detention,¹³⁰ torture, and unauthorised surveillance, citing national security considerations and drawing on the mosaic theory: that when put together, even innocuous pieces of information could provide information to America's enemies. Its secrecy concerns were also evidenced in its reliance on the state secrets doctrine. Its actions are consistent with a variety of possible motives: a good faith determination to protect the homeland, a belief that the payoff for inroads on procedural fairness would be a higher yield of "true positives," fears lest exposure of errors might undermine the legitimacy of the counterterror program, and fears lest exposure cause personal embarrassment.

However, executive enthusiasm for protecting secrets may have waned. In 2009, the attorney general announced measures designed to limit reliance on the doctrine. Invocation of the doctrine would be limited to cases where disclosure "could be expected to cause significant harm to the national security of the United States." The Department of Justice would not defend its invocation to hide violations of law, inefficiency, or administrative error or to prevent embarrassment. Decisions to invoke the privilege would be made initially by an assistant attorney general and would be reviewed by a State Secrets Review Committee. Final decisions would be made by the attorney general, and the Department of Justice would make periodic reports to Congress on cases in which it relied on the privilege.¹³¹ This has not stopped the government from relying on the state secrets doctrine in rendition and torture cases, but in Al-

Aulaqi v Obama, a claim challenging the alleged authorisation of the targeted killing of a US citizen who was outside the country and apparently deeply involved in anti-US terrorism, the government argued that the court did not have to and should not base its decision on the doctrine. The court agreed and dismissed the case on other grounds.¹³²

Elsewhere, executive secrecy concerns were more subdued. One reason is that far less seems to have been at stake. But the governments of the UK, Canada, and Australia all have secrets that they have sought to protect. Another reason is that the courts have generally been receptive to government secrecy claims. Courts are prepared to give terms such as *national security* a reasonably broad interpretation and to give considerable deference to government decisions in relation to whether disclosure would harm national security, although they now require that government claims have a factual basis and adequate evidentiary support.¹³³ The Canadian decision in *Re Charkaoui* is an arguable exception, but one that is explicable in terms of the wording of the relevant legislation.

Courts have generally acknowledged the validity of standard bases for immunity claims. They have acknowledged the importance of the “third party” rule, especially for countries (such as Canada) that are net importers of intelligence.¹³⁴ But the rule does not apply where the government independently acquired the information, where the government has not sought permission to disclose from the provider government, or where the information has been made public by an organ of the provider government.¹³⁵ Courts have acknowledged that the disclosure of apparently innocuous pieces of information may be capable of threatening national security (the mosaic theory).¹³⁶ They have, however, sometimes been sceptical of attempts to base claims for nondisclosure on the theory, and in several cases, they have insisted that arguments based on the theory must be supported by information as to why disclosure of particular pieces of information might contribute to the construction of a mosaic in a way that would undermine security.¹³⁷ Where secrets are inadvertently disclosed, privilege may be claimed in relation to them, but the fact and circumstances of their disclosure is relevant to the balancing exercise required in public interest immunity jurisdictions.¹³⁸ Courts have been sympathetic to claims grounded in the need to protect operational secrets, the identities of informants and operatives, and information given in confidence.¹³⁹

Yet there are limits to deference. Judicial consideration of whether information should be withheld often results in subsequent concessions by the government, coupled with a curial decision that other documents be released.¹⁴⁰ However, lack of deference is asymmetrical: courts have never found governments to have erred in cases where they have contended that information should be disclosed.¹⁴¹

Insofar as courts have addressed the reasons for the overclaiming, they have attributed it to overcaution and to failure even to consider some factors that have an obvious bearing on whether information should be disclosed.¹⁴² However, courts have also commented on the absence of grounds for suspecting that governments overclaimed in order to prevent disclosure of evidence for improper purposes.¹⁴³ But in the UK and Canada, secrecy issues have been the basis for serious conflicts between the security services and the courts.

The UK government fought hard and unsuccessfully to maintain the principle that confidential intelligence from other countries enjoys absolute protection per se. Following the *Al Rawi* decisions, it published a green paper foreshadowing the possibility of legislative changes to enhance the government's capacity to protect its secrets from disclosure in the course of litigation, and in 2013 it secured the passage of legislation to give effect to its proposals.¹⁴⁴ The director of the CSIS was critical of the effects of the 2008 *Charkaoui v Canada* decision: "We were faced with a pretty fundamental dilemma: to disclose information that would have given would-be terrorists a virtual road map to our tradecraft and sources or to withdraw that information from the case, causing a security certificate to collapse."¹⁴⁵ The Australian government has been more successful. Its few applications under the NSIA have enjoyed almost complete success.¹⁴⁶

The Public and Secrets

Even in the United States, there is little evidence as to public opinion in relation to the issue, which suggests that polling agencies and their users do not regard the issue as particularly salient. A 2002 poll suggests a widespread willingness to sacrifice due process for security. Respondents to a 2002 poll were asked whether they thought an American citizen arrested for planning an al-Qaeda terrorist attack in the United States should be held without trial as a "wartime prisoner" or put on trial in the civilian courts. The 42 percent of respondents who favoured trial in the courts were asked what should happen if the government objected that a trial would jeopardise sensitive intelligence. Two-thirds of these respondents still thought the person should be tried, but 29 percent considered he should be held without trial.¹⁴⁷ In a 2006 poll, 48 percent of respondents considered that if disclosure of evidence could put American lives in danger, it would be better to convict defendants on evidence not shown to them than it would be for the defendant to go free because the government withheld the evidence. The remainder were either unsure (11 percent) or considered the defendant should go free (41 percent).¹⁴⁸ Overall, the data suggest that majorities would not object to abridgement of Sixth Amendment rights but that sizeable minorities would. Given the apparently low sa-

lience of this issue, the political capital to be reaped by attacks on the unambiguous constitutional rights at stake would, at most, be minimal, especially given the considerable likelihood that doing so would entail the risk of the legislation being found to be unconstitutional.

Politics and Secrecy

There are scattered pieces of evidence to suggest that the development of the relevant legislation reflects party affiliations, but it is weak. In the United States, the proposed State Secrets Protection Act, which would have narrowed the scope of the state secrets doctrine, was supported in committee by Democrats and opposed by Republicans.¹⁴⁹ In Australia, Labor made attempts to secure amendments to some aspects of the NSIA but generally supported it. The Australian Democrats and the Greens voted against the legislation.

In Canada, the correlates of party were slightly more ambiguous. The Bloc Québécois (BQ) and the New Democrats opposed the Anti-terrorism Act 2001 and dissented from the House of Commons subcommittee report. A proposed amendment to delete the clause by which ministerial certificates could trump freedom of information had the support of the 10 New Democrats and eight BQ members who were present for the vote. It also had support from nine Progressive Conservatives (PCs) and three Canadian Alliance (CA) members of parliament. It was defeated by the votes of 103 Liberals, 33 CA MPs, and a lone PC. There was an almost identical vote in relation to certificates that would trump the Privacy Act. Among the opposition parties, votes roughly reflect their position on a left-right spectrum, but the Liberals' votes are further to the right than one might expect. Moreover, votes on a proposed sunset clause that would have applied to sections of the legislation including the minister's certification power disclosed a somewhat different pattern. The proposal was supported by 10 New Democrats and 16 members of the CA. The government opposed it, supported by seven members of the BQ, eight PCs, and 20 members of the CA. In 2007, a House of Commons subcommittee recommended that a panel of special counsel be established so that entities and charities seeking to challenge their listing or certification could have their interests better represented.¹⁵⁰ The minority, a New Democrat and a member of the BQ, dissented from the report, on the grounds that it should have recommended repeal of the offending provisions (along with the rest of the Anti-terrorism Act).¹⁵¹ As in other contexts, major parties differ little from each other but consistently from smaller parties to their left.

A more robust test of the relevance of party comes from the effects of changes of government. In the United States, the elections of both Bush and Obama have made a difference, albeit one that may also reflect the different

circumstances faced by Clinton and his successors. There have been minor changes in relation to the executive order governing classification criteria and procedures. Executive Order 12958 was made by President Clinton and amended by President Bush. The amendments were relatively subtle, but they facilitated classification by eliminating provisions to the effect that documents were not to be classified or to be classified at a particular level when “significant” doubts existed as to whether they should be. The Bush amendments also made it clear that national defense included defence against transnational terrorism.¹⁵² President Obama’s Executive Order 13526 of 2009 restored the rules against disclosure in the event of “significant doubt” and removed the Bush provisions expanding the scope of “national security” in relation to classifiable documents to include defence against transnational terrorism.¹⁵³ The order included new provisions designed to discourage overclassification and to accelerate review of classification decisions.¹⁵⁴ The administration also announced that it would place only limited reliance on the state secrets doctrine.¹⁵⁵ However, Democrats did not use their majority in the 111th Congress to pass legislation along the lines of the proposed State Secrets Protection Act.

In Australia, the Labor opposition had promised an overhaul of the NSIA on coming to power. It has indeed made extensive amendments to the act, but these have been of a technical nature. It did, however, abolish ministerial certificates as part of an overhaul of freedom of information legislation. Whether a document falls within the category is now a matter for the information commissioner, the Administration Appeals Tribunal, and the courts, but if disclosure could reasonably be expected to cause damage to the security of the commonwealth, the document continues to be exempt from disclosure, regardless of any public interest in disclosure.

In one sense, the UK government’s proposals to amend the public interest immunity laws is consistent with the predispositions hypothesis. It involves a proposal by a Conservative-led coalition to strengthen security at some cost to liberty. Voting was largely along party lines, with Conservatives and their coalition partners and Labour opposing aspects of it. The Conservatives’ Liberal Democrat coalition partners generally supported the government bill in the few House of Commons divisions, but in the House of Lords, Liberal Democrats often supported Labour amendments. However, as we shall see in later chapters, the UK Conservatives have often opposed measures to increase antiterrorism powers and, in government, have taken steps to reduce the scope of some of the more controversial counterterror measures. Moreover the Conservatives’ junior partners, the Liberal Democrats, have a consistent record of relative liberalism in relation to terrorism issues. It seems more plausible to

explain the proposals as a response to the Al Rawi decisions and to the exigencies of being in government.

Conclusions

The rules discussed in this chapter have the potential to work badly. The US state secrets rule means that the protection of state secrets may trump the interests of litigants who would have a strong case but for the rule. The public interest immunity rule seems fairer, but its administration may occasionally make it close to unworkable, and the costs of administering it may be such as to deter claims or to force settlements that bear little relation to the legal merits of the case. In any case, the general rule against the *ex parte* production of evidence means that there will be cases where the protection of secrets will mean that prosecutions are not feasible. One response has been some minor, successful legislative attempts to shift the balance weakly in favour of the government and to devise procedures designed to minimise the risk of disclosure while not prejudicing litigants' legal interests. But there are limits to what the legislation can achieve, assuming that secrets deserve protection and that their disclosure would make decision making more accurate.

The scope of the problem is unclear. Given the rarity of domestic terrorist attacks, it is not a serious one, at least as far as governments are concerned. Moreover, as we shall see in chapter 7, governments have normally been able to achieve convictions in terrorism cases. This does not preclude the possibility of there having been cases where "offenders" could not be prosecuted without disclosure. But if this is so, none of the villains has subsequently committed a terrorist act within the jurisdiction. Nonetheless, perceived problems arising from open trial requirements are among the factors that have encouraged interest in means of bypassing the courts and that have tempted governments to resort to the use of extralegal measures in the fight against terrorism, which themselves become secrets that governments wish to protect.